F. #2012R00103

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

15 M 103

- X

IN THE MATTER OF AN APPLICATION
FOR A SEARCH WARRANT FOR:

THE PREMISES KNOWN AND DESCRIBED
AS THE DROPBOX ACCOUNT
ASSOCIATED WITH ELECTRONIC MAIL
ADDRESS "DUBOVOY1@GMAIL.COM"

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH
WARRANT

- X

EASTERN DISTRICT OF NEW YORK, SS:

Jonathan Polonitza, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is located in THE PREMISES KNOWN AND DESCRIBED AS THE DROPBOX ACCOUNT ASSOCIATED WITH ELECTRONIC MAIL ADDRESS "dubovoy1@gmail.com" (the "SUBJECT PREMISES") subscriber/profile information, file transmission information, subject headings, to/from information, folders and file content (including all of the foregoing for deleted files), as described more fully in Attachment B, which constitute evidence, fruits and instrumentalities of the unlawful hacking of newswire services to trade upon misappropriated insider stock information occurring in the Eastern District of New York and elsewhere, in violation of 18 U.S.C. §§ 371, 1030, 1343, 1348 and1349, by Arkadiy Dubovoy, Igor Dubovoy, Pavel Dubovoy, Vitaly Korchevsky,_Ivan Turchynov, _Oleksandr

Ieremenko, Vladislav Khalupsky, Leonid Momotok, Georgij Golovan, Gennady Arkhipov, Victoria Bulkina, Martin Oherd, Evgeniy Petrakov and Dmitry Voronin, among others.

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been employed by the FBI since January 2011. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for crimes related to the unlawful accessing and use of computer media. I am one of the case agents with primary responsibility for this investigation. While working for the FBI, I have participated in numerous investigations of criminal activity, including bank fraud, securities fraud, corporate fraud, insider trading, money laundering schemes, and other types of schemes. During the course of these investigations, I have conducted or participated in surveillance, undercover transactions, the execution of search warrants, debriefings of informants, and reviews of taped conversations and financial records. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. I am familiar with the information contained in this affidavit based on my personal participation in the investigation, my review of documents, my training and experience, and my discussions with other law enforcement personnel concerning the

[1] Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

investigation. In addition, statements in this affidavit attributable to individuals are set forth in substance and in part.

3. The FBI and the United States Secret Service are investigating the unlawful hacking of newswire services to trade upon misappropriated insider stock information in the Eastern District of New York, the District of New Jersey and abroad. This investigation, described more fully below, has revealed that an individual using the email address Dubovoy1@gmail.com did knowingly engage in a conspiracy to hack into companies and trade securities upon the misappropriated information. The investigation to date has established that the members of this conspiracy were storing such misappropriated information using the SUBJECT PREMISES, a Dropbox file sharing account. The evidence indicates that I submit that there is probable cause to believe there is evidence, fruits, and instrumentalities of the violations of in violation of 18 U.S.C. §§ 371, 1030, 1343, 1348 and1349 located in the SUBJECT PREMISES.

I. BACKGROUND

4. The investigation has identified an international conspiracy of traders who made money trading securities based on private corporate information that they obtained through an unauthorized criminal intrusion (or "hacking") into the computer servers of newswire companies such as PR Newswire ("PRN"). As shown by forensic analysis of the computer media and the trading activity, these unauthorized criminal intrusions, or "hacks," go as far back as 2008. The hackers have continued to assault the PRN networks as recently as April 2014. The most recent hack were designed to trick PRN employees into activating links that transmitted malicious software from a Dropbox account.

A. The Initial PRN Hack

5. Law enforcement is investigating an international network of traders who may have made money trading securities based on private corporate information that they obtained through an unauthorized criminal intrusion (or "hacking") into at least one computer server of PR Newswire, a U.S. company. PR Newswire publishes press releases for other companies, many of which are publicly traded on securities exchanges.

6. PRN is a United States company that provides marketing and communications services for other companies, many of which are publicly traded on various exchanges. Among other services, PRN receives confidential non-public information from publicly traded companies in the forms of press releases and then, at the time of the client company's choosing, PRN distributes the press releases ("PRN Releases") to the public. Those PRN Releases are held by PRN in its computers and servers until the contracted time of distribution. Until the contracted distribution time, PRN is contractually bound to keep the content of the press releases confidential and non-public.

7. As a result of the hack, the members of this conspiracy were able to connect regularly to the web server and download press releases from newswire services such as PRN before those press releases were released to the general public. Because those press releases often contained important and not yet public information about corporations trading on United States stock exchanges, including earnings figures, the members of the conspiracy were able to make a profit by secretly accessing and trading on the information before it was made public.

8. During an examination of the hacked PRN web server, investigators found a PHP script that had been placed on the server without authorization. PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language. Thus, an unauthorized PHP script is an unauthorized program that can run undetected within the hacked PRN server. The unauthorized PHP script could be accessed and run from any Internet-connected computer in the world by typing in a long web address that included the PHP script's name. The script was programmed not to respond unless the web address included a long string of letters and numbers.

9. An IP address is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

10. Web server logs recovered from the hacked server show a series of repeated and regular accesses to that PHP script. Several of those accesses came from the following IP addresses: 94.100.218.42 (the "First Hack IP"), which is associated with known hacker Ivan Turchynov.

11. The investigation has revealed that hundreds of stolen PRN Releases were sent from the First Hack IP to other email accounts. As of this date, the investigation has identified more than a hundred traders who appear, based upon our analysis, to have traded on the hacked information.

II. SUBJECT PREMISES

B. The First Hack IP's Connections to Igor Dubovoy

20. Investigation has also revealed that, approximately 160 times between July 2011 and June 2013, the First Hack IP was used to access United States TD Ameritrade brokerage account number 862-194751 (the "Dubovoy TD Ameritrade Account"). TD Ameritrade provides online brokerage services to customers who maintain an account with the company, such as the controllers of the Dubovoy Brokerage Account. According to subpoenaed account opening documents, Arkadiy Dubovoy and Igor Dubovoy, both of whom live in Alpharetta, Georgia, are the official controllers of the Dubovoy TD Ameritrade Account.

21. In a two-minute window on the afternoon of Feb. 21, 2012, the Dubovoy TD Ameritrade Account made four trades in advance of publication of PRN releases. All of those trades correctly applied the hacked new release information. Indeed, approximately 80 trades from this account utilize hacked news releases.

22. Similarly, the First Hack IP also accessed Fidelity brokerage account X77-566216 ("Dubovoy Fidelity Account"). Fidelity provides online brokerage services to customers who maintain an account with the company, such as the controllers of the Dubovoy Fidelity Account, which is again associated with Arkadiy Dubovoy and Igor Dubovoy of Alpharetta, Georgia.

23. An analysis of subpoenaed trading records shows that the Dubovoy Fidelity Account also traded in advance of dozens of other hacked news releases.

24. "APD Developers Inc." is a company operated by Arkadiy and Igor Dubovoy. According to records received from TD Ameritrade, Igor and Arkadiy Dubovoy

also maintained a brokerage account with TD Ameritrade that was opened with the name of "APD Developers Inc." (the "APD Trading Account"). The APD Trading Account remained open until in or about 2012, when TD Ameritrade closed the account due to Dubovoy's suspected insider trading.

25. A trading analysis indicated that the Dubovoy TD Ameritrade, Dubovoy Fidelity, APD Trading Account and others engaged in hundreds of trades upon misappropriated information resulting in millions of dollars of profits.

26. One of Igor Dubovoy's personal email accounts is the Dubovoy1@gmail.com. Dubovoy1@gmail.com was the email account used to establish the same Dubovoy TD Ameritrade Account and Dubovoy Fidelity Account that were both accessed by the First Hack IP. Igor Dubovoy's email account (Dubovoy1@gmail.com) was also used to communicate with TD Ameritrade and Fidelity on issues or questions relating to Dubovoy TD Ameritrade Account and Dubovoy Fidelity Account. These accounts were also accessed by the First Hack IP (94.100.218.42).

C. The Connections Between Igor Dubovoy and the SUBJECT PREMISES

27. Dropbox, Inc., headquartered in San Francisco, California, operates a popular file hosting service called "Dropbox." Dropbox allows users to create a special folder on their computers, which is synchronized so that it appears to be the same folder (with the same contents) regardless of which computer is used to view it. Files placed in this folder are also accessible via the Dropbox website and mobile applications.

28. Based upon Dropbox, Inc.'s records, Igor Dubovoy's name, home address, Dubovoy1@gmail.com email address and credit card were used to establish a Dropbox account.

29. Further investigation has revealed that IP address 98.66.187.101 (the "First Dropbox IP") has been utilized to access the Dubovoy TD Ameritrade Account and the Dubovoy Fidelity Account. The First Dropbox IP also accessed brokerage accounts held by Arkadiy Dubovoy, APD Developers and M&I Advising Associate LLC[1]. In addition to all of these contacts shared with the hackers and traders, the First Dropbox IP also accessed the SUBJECT PREMISES.

30. Similarly, additional investigation has revealed that IP address 24.30.50.196 (the "Second Dropbox IP") has been utilized to access the Dubovoy TD Ameritrade Account and the Dubovoy Fidelity Account. The Second Dropbox IP also accessed brokerage accounts held by Arkadiy Dubovoy, APD Developers (owned by Arkadiy Dubovoy) and M&I Advising Associates LLC. The Second Dropbox IP also accessed the SUBJECT PREMISES.

31. Additional investigation has also revealed that IP address 23.31.147.134 (the "Third Dropbox IP") accessed brokerage accounts held by Arkadiy Dubovoy, and APD Developers. The Third Dropbox IP also accessed the SUBJECT PREMISES.

B. Other Connections Between the Hack and the SUBJECT PREMISES

32. Beginning in November 2014, law enforcement officials have been debriefing a Ukraine national with knowledge of the PRN Hack ("CS-1"). CS-1 described how hackers would share stolen newswire information in their individual DropBox accounts. CS-1 voluntarily provided access to his own DropBox account. A forensic examination of

[1] APD Developers and M&I Advising Associates LLC are entities owned and controlled by Arkadiy Dubovoy and Igor Dubovoy.

that Dropbox account confirmed that misappropriated information from PRN had passed through CS-1's DropBox account.

33. Based upon all of the above information, and my experience working in cases like this, I think that it is very likely that there is evidence of the PRN hack and its connected trades located in the SUBJET PREMISES. While CS-1's DropBox account had no immediate contacts with the SUBJECT PREMISES, I still think that it is very likely that, given the various contacts between the SUBJECT PREMISES, the confirmed hackers and the trading accounts, the SUBJECT PREMISES contain evidence of hacking activity and its related trades.

III. TECHNICAL BACKGROUND

34. The SUBJECT PREMISES is file hosting service account which is hosted by Dropbox, Inc. (hereinafter, the "file hosting provider"). In my training and experience, I have learned that the file hosting provider provides a variety of online services, including file hosting service accounts, to the general public. The file hosting provider allows subscribers to obtain accounts at the domain name gmail.com, such as the email account listed in Attachment A. Subscribers obtain an account by registering with the file hosting provider. During the registration process, the file hosting provider asks subscribers to provide basic personal information. Therefore, the computers of the file hosting provider are likely to contain stored electronic communications and information concerning subscribers and their use of the file hosting provider's services, such as account access information, and account application information.

35. In general, a file is sent hosted by the file hosting provider's subscriber is stored in the subscriber's "Dropbox" on the file hosting provider's servers. If the

subscriber does not delete the file, the message can remain on the file hosting provider's servers indefinitely. Even if the subscriber deletes the file, it may remain in the subscriber's "trash" folder or otherwise remain accessible to the subscriber.

36. When the subscriber submits a file to the service, it is initiated at the user's computer, transferred via the Internet to the file hosting provider's servers, and then transmitted to its end destination. The file hosting provider often saves a copy of the file sent. Unless the sender of the file specifically deletes the file from the file hosting provider's server, the file can remain on the system indefinitely.

37. A submitted file typically includes the content of the file, source and access, the date and time at which the file was sent, the size and length of the file, and IP address information about every individual who accesses the submitted file. If a Dropbox user begins to submit a file but does not complete the action, that file may also be saved by the file hosting provider but may not include all of these categories of data.

38. In general, file hosting providers like Dropbox, Inc. ask each of their subscribers to provide certain personal identifying information when registering for a Dropbox account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

39. File hosting providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such

as logging into the account via the file hosting provider's website or via applications), and other log files that reflect usage of the account. In addition, file hosting providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. An IP address is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

40. In some cases, email account users will communicate directly with a file hosting provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. File hosting providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

41. In my training and experience, evidence of who was using an file hosting account may be found in the IP addresses, the registration materials and the content of the hosted pictures and files.

IV. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

42. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require the file hosting provider to disclose to the government copies of the records and other information (including the content of

communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

V. CONCLUSION

43. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in the control of the file hosting provider evidence of crimes exists. Accordingly, a search warrant is requested.

44. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

45. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

46. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing these documents is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations, and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other criminals as they deem appropriate, e.g., by posting them publicly through online forums. Therefore, premature disclosure of the contents of this affidavit and related documents will seriously jeopardize the investigation, including by giving targets an opportunity to flee or

continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, and notify confederates.

47. Pursuant to 18 U.S.C. § 2705(b) and for the reasons stated above, it is further requested that the Court issue an Order commanding Dropbox, Inc. not to notify any person (including the subscribers or customers of the account listed in the attached warrant) of the existence of the attached warrant until further order of the Court.

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS THE DROPBOX ACCOUNT ASSOCIATED WITH ELECTRONIC MAIL ADDRESS "dubovoy1@gmail.com"

IT IS FURTHER REQUESTED that all papers submitted in support of this application, including the application and search warrant, be sealed until further order of the Court.

Jonathan Polonitza
Special Agent
Federal Bureau of Investigation

Sworn to before me this
3 day of February, 2015

S/ Vera Scanlon

THE HONORABLE VERA M. SCANLON
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Dropbox account registered to "dubovoy1@gmail.com" that is stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., a company that accepts service of legal process at:

Dropbox, Inc.
Attention: Legal Department
185 Berry Street, 4th Floor
San Francisco, CA 94043
Fax: (415) 789-4485

ATTACHMENT B
Particular Things to be Seized

I. Search Procedure

A. Within fourteen days of the search warrant's issue, the warrant will be served on Dropbox, Inc. personnel, who will identify the accounts and files to be searched, as described in Section II below.

B. Dropbox, Inc. will then create an exact electronic duplicate of these accounts and files ("the account duplicate").

C. Dropbox, Inc. will provide the account duplicate to law enforcement personnel.

D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.

E. Law enforcement personnel may review the account duplicate, even if Dropbox, Inc. produced it after fourteen days from the warrant's issue, subject to the following limitations. If Dropbox, Inc. provided data that was created after fourteen days from the warrant's issue ("late-created data"), law enforcement personnel may view all late-created data that was created by Dropbox, Inc., including subscriber, IP address, logging, and other transactional data, without a further order of the Court. Law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as e-mail, absent a follow-up warrant.

II. Information to be disclosed by Dropbox, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs or other information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

A. The contents of all files and communications associated with the account, including stored or preserved copies of files and communications sent to and from the account, the source and destination addresses associated with each files and communication, the date and time at which each files and communications was sent, and the size and length of each files and communication;

B. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

C. The types of service utilized;

D. All records or other information stored at any time by an individual using the account; and

E. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

Pursuant to Rule 41(f)(1)(B), the government will retain a copy of the electronically stored information that was seized or copied for the purpose of evidentiary authentication and any potential discovery obligations in any related prosecution. All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 371, 1030, 1343, 1348 and1349, those violations involving Arkadiy Dubovoy, Igor Dubovoy, Pavel Dubovoy, Vitaly Korchevsky, Ivan Turchynov, Oleksandr Ieremenko, Leonid Momotok, Georgij Golovan, Gennady Arkhipov, Victoria Bulkina, Martin Oherd, Evgeniy Petrakov and Dmitry Voronin, among others, and occurring after March 1, 2009, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

A. The unlawful hacking of newswire services to trade upon misappropriated insider stock information occurring in the Eastern District of New York and elsewhere, in violation of 18 U.S.C. §§ 371, 1030, 1343, 1348 and1349.

B. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.